CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 15-82
- After this Amendment: Claims 15-82

Non-Elected, Canceled, or Withdrawn claims: None

Amended claims: 39, 65, and 73

New claims: None

Claims:

1–14. (Canceled)

15. (Previously Presented) A method of protecting media content stored on a storage medium, the method comprising:

creating a first session on the medium, the first session containing digital data stored in a first format and representing all or substantially all of the media content, the digital data in the first session being readable by an electronic device configured to read digital data in the first format;

creating a second session on the medium, the second session containing digital data stored in a second format and representing all or substantially all of the media content, the digital data in the second session being readable by a

media player associated with a computing device and configured to read the digital data in the second format;

including on the second session at least one digital rights management license describing allowed uses for the digital data;

including on the second session digital rights management software;

encrypting the digital data in the second session so that the digital rights management software does not grant access to the digital data stored in the second session unless the digital rights management software determines that a requested access complies with the allowed uses described in the at least one digital rights management license; and

preventing the media player associated with the computing device configured to read the digital data in the second format from accessing the digital data in the first format.

16. (Previously Presented) The method of claim 15, wherein encrypting the data comprises:

separating the media content into packets of data;

encrypting the packets;

storing the encrypted packets to the medium; and

storing at least one decryption key on the medium such that the digital rights management software, when executed by a computer, causes the computer to use the at least one decryption key to decrypt the packets.

17. (Previously Presented) The method of claim 16, wherein encrypting the data further comprises:

creating at least two encryption keys;

for every encryption key, encrypting at least one packet with that key;

encrypting every packet with the at least two encryption keys; and

wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

18. (Previously Presented) The method of claim 17, wherein the encryption keys are symmetric, and wherein the method further comprises:

generating at least one protection encryption key for each of the at least two encryption keys;

encrypting each encryption key with an associated protection encryption key;

storing the at least one encrypted encryption key on the medium; and

storing at least one protection decryption key on the medium, such that the at least one protection decryption key can be used to decrypt the at least one encryption key.

19. (Previously Presented) The method of claim 18, wherein:

the at least one protection encryption key comprises a generic protection decryption key and a unique protection encryption key; and

the at least one protection decryption key comprises a generic protection decryption key and a unique protection decryption key.

20. (Previously Presented) The method of claim 18, wherein storing the at least one protection decryption key comprises integrating the protection decryption key inside the digital rights management software.

21. (Previously Presented) The method of claim 15, wherein the digital rights management software is tamper-resistant.

22. (Previously Presented) The method of claim 21, further comprising:

storing a binding identifier on the medium, wherein the binding identifier is associated with the at least one digital rights management license, and is used by the digital rights management software to determine whether or not to allow the requested access to the digital data in the second session, and wherein the binding identifier cannot be duplicated onto another storage medium.

23. (Previously Presented) The method of claim 22 wherein:

storing the binding identifier comprises encrypting together the at least one license and a copy of the binding identifier that is associated with the at least one license; and

the digital rights management software compares a decrypted copy of the binding identifier to the binding identifier present on the medium before allowing the requested access.

24. (Previously Presented) The method of claim 22, wherein:

storing the binding identifier comprises:

creating a license encryption key from the binding identifier; and

encrypting the at least one license with the encryption key; and

the digital rights management software decrypts the at least one license using a decryption key created from the binding identifier to determine whether or not to allow the requested access to the digital data in the second session.

25. (Previously Presented) The method of claim 15, wherein:

the digital data on the first session comprises a plurality of separate audio recordings;

the at least one digital rights management license comprises a plurality of digital rights management licenses; and

at least one of the plurality of digital rights management licenses describes allowed uses for a specific recording.

26. (Original) The method of claim 15, wherein the medium is a compact disc.

27. (Previously Presented) A compact disc, comprising:

a first session readable by a compact disc player;

first data representing all or substantially all media content on the compact disc, the first data stored on the first session and protected so that the first data cannot be decoded into a renderable media presentation by an optical media drive;

a second session readable by an optical media drive;

second data representing all or substantially all of the media content on the compact disc, the second data stored on the second session and encrypted so that the second data cannot be decoded into a renderable media presentation by the compact disc player;

at least one digital rights management license, written to the second session, and describing allowed uses for the second data;

digital rights management software stored on the second session that, when executed by a computer, causes the computer to use the digital rights management license to determine whether or not a requested use of the second data is allowed, and to prevent the requested use of the second data if the license does not permit the requested use;

at least one decryption key stored on the second session and used by the digital rights management software to decrypt the second data.

28. (Previously Presented) The compact disc of claim 27, wherein the encrypted second data comprises a plurality of encrypted packets of data.

29. (Original) The compact disc of claim 28, wherein the plurality of encrypted packets are encrypted with a plurality of encryption keys, and wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

30. (Previously Presented) The compact disc of claim 27, wherein the at least one decryption key is integrated inside the digital rights management software.

31. (Previously Presented) The compact disc of claim 27, wherein the digital rights management software is tamper resistant.

32. (Previously Presented) The compact disc of claim 31, further comprising:

a binding identifier stored on the compact disc, associated with the at least one digital rights management license, and used by the digital rights management software to determine whether or not to allow the requested use of the second data, wherein the binding identifier cannot be duplicated onto another compact disc.

33. (Previously Presented) The compact disc of claim 32, further comprising:

the at least one license and a copy of the binding identifier encrypted together and stored on the second session; and

wherein the digital rights management software, when executed by the computer, also causes the computer to compare a decrypted copy of the binding identifier to the binding identifier present on the disc before allowing a requested use of the second data.

34. (Previously Presented) The compact disc of claim 32, wherein:

the at least one license is encrypted using an encryption key created by using the binding identifier as a seed; and

the digital rights management software, when executed by the computer, also causes the computer to decrypt the at least one license using a decryption key created from the binding identifier to determine whether or not to allow a requested use of the second data.

35. (Previously Presented) The compact disc of claim 27, wherein:

the second data on the second session comprises a plurality of separate audio recordings;

the at least one digital rights management license comprises a plurality of digital rights management licenses; and

at least one of the plurality of digital rights management licenses describes allowed uses for a specific audio recording.

36. (Previously Presented) The compact disc of claim 35, wherein the plurality of digital rights management licenses contain a license describing uses for a plurality of the audio recordings in addition to the at least one license that describes uses for a specific audio recording.

37. (Previously Presented) The compact disc of claim 27, further comprising at least one validation code associated with the digital rights

management software wherein the at least one code represents a cryptographically-signed hash of a canonical representation of at least one section of the digital rights management software code, and wherein the digital rights management software, when executed by the computer, causes the computer to detect tampering or replacement of the at least one section of code at the time the code is executed by performing a runtime hash of the at least one section of code and comparing the runtime hash to the stored cryptographically-signed hash.

38. (Previously Presented) The compact disc of claim 27 further comprising protected playback software that, when executed by the computer, causes the computer to play the second data.

39. (Currently Amended) A system for protecting media content, the system comprising:

a computing device;

media content stored on the computing device;

at least one digital rights management license stored on the computing device and describing allowed uses for the media content;

digital rights management software stored on the computing device and that, when executed by the computing device, causes the computing device to use the digital rights management license to determine whether or not a requested use of the ~~second data~~ media content is allowed, and to prevent the

requested use of the ~~second data~~ media content if the license does not permit the requested use; and

wherein the media content, the at least one digital rights management license, and the digital rights management software were installed on the computing device from a single storage medium that contained the content, the license, and the software.

40. (Previously Presented) The system of claim 39, further comprising:

a first identifier associated with the at least one digital rights management license;

a hard drive, coupled to the computing device;

a second identifier, stored on the hard drive; and

wherein the digital rights management software, when executed by the computing device, causes the computing device to compare the first identifier to the second identifier before allowing a requested use of the media content.

41. (Original) The system of claim 39, wherein the digital rights management software comprises a generic module and a unique module.

42. (Previously Presented) The system of claim 39, further comprising:

at least one validation code corresponding to at least one predetermined software module; and

validation software that, when executed by the computing device, causes the computing device to compute at least one checksum for the at least one

software module and compare the at least one checksum against the validation code to determine if the at least one predetermined software module should be trusted.

43. (Previously Presented) The system of claim 42, wherein:

the at least one validation code is a cryptographically-signed hash of a canonically-ordered series of bytes from the at least one predetermined software module; and

comparing the at least one checksum against the validation code comprises:

decrypting the cryptographically-signed hash;

performing a hash on the at least one software module; and

comparing the results of the two hashes to see if they match.

44. (Previously Presented) The system of claim 39, wherein the storage medium is a compact disc.

45. (Previously Presented) A method of transferring digital data from a removable storage medium to a storage device coupled to a computing device, the method comprising:

copying the digital data from the removable storage medium to the storage device;

copying at least one digital rights management license from the removable storage medium to the storage device, the digital rights management license describing types of access that are allowed for the digital data;

copying digital rights management software from the removable storage medium to the storage device, wherein the digital rights management software, when executed by the computing device, causes the computing device to use the at least one digital rights management license to determine whether or not an access to the digital data is permitted.

46. (Previously Presented) The method of claim 45, further comprising:

determining whether or not the computing device has secure playback software that can read the digital data; and

installing secure playback software if the computing device does not have the software.

47. (Previously Presented) The method of claim 45, further comprising encrypting the at least one digital rights management license, and wherein the copied digital rights management software, when executed by the computing device, causes the computing device to deny access to the digital data on the storage device unless the at least one digital rights license is decrypted.

48. (Previously Presented) The method of claim 47, wherein encrypting the at least one digital rights management license comprises:

generating a binding identifier for the storage device;

storing the identifier on the storage device;

generating an encryption key from the binding identifier;

encrypting the at least one digital rights management license using the generated encryption key; and

wherein the digital rights management software, when executed by the computing device, causes the computing device to use the binding identifier to create a decryption key for the at least one license.

49. (Previously Presented) The method of claim 45, wherein the removable storage medium is a compact disc.

50. (Previously Presented) A method of playing media content stored on a removable storage medium the method comprising:

reading digital data stored in a second format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a first format that also represents all or substantially all of the media content;

determining from at least one digital rights management license whether or not playback of the digital data stored in the second format is allowed.

51. (Previously Presented) The method of claim 50, wherein the removable storage medium is a compact disc.

52. (Previously Presented) The method of claim 50, further comprising authenticating digital rights management software that, when executed by a computer, causes the computer to use the at least one digital rights management license to determine whether or not to allow playback of the digital data.

53. (Previously Presented) The method of claim 78, wherein the encrypted data comprises a plurality of encrypted packets of data.

54. (Previously Presented) The method of claim 53 wherein decrypting the data comprises:

locating at least one decryption key on the removable storage medium; and

using the at least one decryption key to decrypt the packets of data.

55. (Previously Presented) The method of claim 54, wherein:

the at least one decryption key is itself encrypted with a protection encryption key; and

the removable storage medium contains at least one protection decryption key to decrypt the at least one encrypted decryption key.

56. (Previously Presented) The method of claim 55, wherein:

the protection encryption key comprises a generic protection encryption key and a unique protection encryption key; and

the at least one protection decryption key comprises a generic protection decryption key and a unique protection decryption key.

57. (Previously Presented) The method of claim 55, wherein the at least one decryption key is symmetric.

58. (Previously Presented) The method of claim 55, further comprising:

generating a symmetric playback protection key;

encrypting the at least one decryption key with the symmetric key; and

wherein decrypting the encrypted packets of digital data stored in the second format further comprises decrypting the at least one encrypted decryption key prior to decrypting the packets of data.

59. (Previously Presented) The method of claim 58, further comprises:

playing the encrypted digital data stored in the second format; and

deleting the at least one decryption key and the decrypted packets of data from memory.

60. (Previously Presented) A method of transferring digital data stored on a removable storage medium to an external device, the method comprising:

loading digital rights management software from the medium;

retrieving a digital rights management license from the medium; and

using the digital rights management license to determine whether or not a transfer of the digital data to the external device is allowed.

61. (Previously Presented) The method of claim 60, wherein the removable storage medium is a compact disc.

62. (Previously Presented) The method of claim 60, further comprising authenticating the digital rights management software.

63. (Original) The method of claim 60, wherein the external device is a compact disc burner.

64. (Original) The method of claim 60, wherein the external device is a portable audio player.

65. (Currently Amended) The method of claim 79, further comprising translating the at least a portion of the digital data into a format that the [[the]] external device can read.

66. (Previously Presented) The method of claim 64, further comprising transferring the digital rights management software and the digital rights management license from the removable storage medium to the portable audio player.

67. (Previously Presented) The method of claim 66, wherein:

the portable audio player contains digital rights management software that is different than the software loaded from the removable storage medium; and

the method further comprises:

translating the digital rights management license into a format that the software already on the portable audio player can read; and

transferring the translated digital rights management license to the portable audio player.

68. (Previously Presented) A removable computer readable storage medium storing media content and a program that, when executed by a computer, causes the computer to:

read digital data stored on the medium in a second format and representing all or substantially all of the media content, wherein the medium also contains digital data stored in a first format that also represents all or substantially all of the media content;

locate a digital rights management license stored on the medium; and

using the digital rights management license to determine whether or not a requested use of the digital data stored in the second format is allowed.

69. (Original) The medium of claim 68, wherein the medium is a compact disc.

70. (Previously Presented) The medium of claim 68, wherein the stored program further causes the computer to authenticate the program.

71. (Previously Presented) The medium of claim 80, wherein the encrypted data comprises encrypted packets of data.

72. (Previously Presented) The medium of claim 71, wherein the stored program further causes the computer to:

locate a decryption key on the medium; and

decrypt the packets of data using the decryption key.

73. (Currently Amended) The medium of claim 72, wherein:

the decryption key is itself encrypted with a protection encryption key; and

the stored program further causes the computer to use the protection decryption key to decrypt the encrypted decryption key[[; and]].

74. (Previously Presented) The medium of claim 73, wherein:

the protection encryption key comprises a generic protection encryption key and a unique protection encryption key; and

the protection decryption key comprises a generic protection decryption key and a unique protection decryption key.

75. (Previously Presented) The medium of claim 73, wherein the decryption key is symmetric.

76. (Previously Presented) The medium of claim 73, wherein the stored program further causes the computer to:

generate a symmetric playback protection key;

encrypt the decryption key with the symmetric key; and

decrypt the encrypted decryption key prior to decrypting the packets of data.

77. (Previously Presented) The medium of claim 76, wherein the stored program further causes the computer to:

play the encrypted digital data stored in the first format, and

delete the decryption key and the decrypted packets of data from memory.

78. (Previously Presented) The method of claim 50 wherein:

the digital data stored in the first format is encrypted, and

the method further comprises decrypting the encrypted data.

79. (Previously Presented) The method of claim 60 further comprising transferring at least a portion of the digital data to the external device in response to the determination that the digital rights management license permits the transfer.

80. (Previously Presented) The medium of claim 68, wherein:

The digital data stored in the second format is encrypted, and

the stored program further causes the computer to decrypt the encrypted data.

81. (Previously Presented) A method of playing media content stored on a removable storage medium the method comprising:

reading digital data stored in a first format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a second format that also represents all or substantially all of the media content;

preventing an audio player configured to read the digital data stored in the second format from reading the digital data in the first format.

82. (Previously Presented) The method of claim 81 wherein the first format comports to the Redbook compact disc standard.